

FORM PTO-1390  
(REV. 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

**TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371**

2085-00200

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)

**09/937634**  
NOT YET ASSIGNED

INTERNATIONAL APPLICATION NO.  
PCT/SG99/00020

INTERNATIONAL FILING DATE  
22 March 1999

PRIORITY DATE CLAIMED  
22 March 1999

TITLE OF INVENTION  
METHOD AND APPARATUS FOR ENCRYPTING AND DECRYPTING DATA

APPLICANT(S) FOR DO/EO/US  
Feng BAO et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below. (English translation not necessary as it was originally filed in English.)
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☐ is attached hereto (required only if not communicated by the International Bureau).
  - b. ☒ has been communicated by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
  - a. ☐ is attached hereto.
  - b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are attached hereto (required only if not communicated by the International Bureau).
  - b. ☐ have been communicated by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

**Items 11 to 20 below concern document(s) or information included:**

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
14. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
15. ☐ A substitute specification.
16. ☒ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information:  
International Application as published (cover sheet only); PCT Form PCT/IPEA/402; Form PCT/IB/308; PCT Request Form; International Search Report; and an acknowledgment postcard.

U.S. APPLICATION NO. (if known, see 37 CFR 1.53)  
NOT REASSIGNED 69/937634INTERNATIONAL APPLICATION NO  
PCT/SG99/00020ATTORNEY'S DOCKET NUMBER  
2085-00200


21. <input checked="" type="checkbox"/> The following fees are submitted:				CALCULATIONS PTO USE ONLY	
<b>BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):</b> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO. .... <b>\$1000.00</b>  International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... <b>\$860.00</b>  International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... <b>\$710.00</b>  International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) ..... <b>\$690.00</b>  International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) ..... <b>\$100.00</b> <b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b>					
Surcharge of <b>\$130.00</b> for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(e)).					
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	46 - 20 =	26	x <b>\$18.00</b>	\$ 468.00	
Independent claims	4 - 3 =	1	x <b>\$80.00</b>	\$ 80.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ <b>\$270.00</b>	\$ 00.00	
<b>TOTAL OF ABOVE CALCULATIONS =</b>				\$ 1,548.00	
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.				\$ 774.00	
<b>SUBTOTAL =</b>				\$ 774.00	
Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				\$ 00.00	
<b>TOTAL NATIONAL FEE =</b>				\$ 774.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). <b>\$40.00</b> per property +				\$ 40.00	
<b>TOTAL FEES ENCLOSED =</b>				\$ 814.00	
				Amount to be refunded:	\$
				charged:	\$ 814.00

- a. ☐ A check in the amount of \$ \_\_\_\_\_ to cover the above fees is enclosed.
- b. ☒ Please charge my Deposit Account No. 03-2769 in the amount of \$ 814.00 to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 03-2769. A duplicate copy of this sheet is enclosed.
- d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

**NOTE:** Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:  
Jonathan M. Harris, Esq.  
CONLEY, ROSE & TAYON, P.C.  
P.O. Box 3267  
Houston, Texas 77253-3267  
United States of America

DATE: September 24, 2001

  
SIGNATURE  
Jonathan M. Harris  
NAME  
Reg. No. 44,144  
REGISTRATION NUMBER

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Feng BAO et al.	§	
		§	
Serial No.:	Not Yet Assigned	§	Group Art Unit: UNKNOWN
		§	
Filed:	Concurrently Herewith	§	Examiner: UNKNOWN
		§	
For:	Method And Apparatus For	§	Express Mail Label No. EL915360557US
	Encrypting And Decrypting Data	§	

**PRELIMINARY AMENDMENT**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Att'y. Docket No. 2085-00200  
Client Ref. No. KRD-P004US(WO)  
Date: September 24, 2001

Sir:

This paper is filed concurrently with the National Phase Entry patent application. Prior to examining this case, the Examiner is requested to enter the following amendments and consider the accompanying remarks.

**IN THE CLAIMS:**

Please amend claims 4, 5, 8, 11-13, 17, 20-23, 27, 28, 31, 34-36, 40, and 43-46 by replacement with the following rewritten claims. A marked up version of the amended claims, showing the changes by underlining of the added text and bracketing of the deleted text, is appended hereto.

- 1 4. A method according to claim 1 wherein step (e) includes outputting the size of the
- 2 corresponding data segment.
  
- 1 5. A method according to claim 1 wherein said first function includes a cryptographic
- 2 pseudo random generator.

1 8. A method according to claim 1 wherein said accessory data strings are derived  
2 from various sources.

1 11. A method according to claim 1 wherein said second function includes an  
2 encryption function of a symmetric key cipher.

1 12. A method according to claim 1 wherein said second function includes an  
2 encryption function of a block cipher operating in a well known mode, such as Electronic  
3 Code Book mode.

1 13. A method according to claim 1 wherein said second function includes an  
2 encryption function resulting from combined use of more than one symmetric key cipher.

1 17. A method according to claim 14 wherein said first function includes a  
2 cryptographic pseudo random generator.

1 20. A method according to claim 14 wherein said accessory data strings include two  
2 parts, one part being derived by the decrypting party in a predetermined fashion from  
3 available sources prior to decrypting said *i*th ciphertext segment and the other part not  
4 being derived by, and therefore being received by, the decrypting party prior to decrypting  
5 said *i*th ciphertext segment.

1 21. A method according to claim 14 wherein said second function includes a  
2 decryption function of a symmetric key cipher.

1 22. A method according to claim 14 wherein said second function includes a  
2 decryption function of a block cipher operating in a well known mode, such as Electronic  
3 Code Book mode.

1 23. A method according to claim 14 wherein said second function includes a  
2 decryption function resulting from a combined use of more than one symmetric key cipher.

1 27. Apparatus according to claim 24 wherein said means for outputting is adapted for  
2 outputting the size of the corresponding data segment.

1 28. Apparatus according to claim 24 wherein said first function includes a  
2 cryptographic pseudo random generator.

1 31. Apparatus according to claim 24 wherein said accessory data strings are derived  
2 from various sources.

1 34. Apparatus according to claim 24 wherein said second function includes an  
2 encryption function of a symmetric key cipher.

1 35. Apparatus according to claim 24 wherein said second function includes an  
2 encryption function of a block cipher operating in a well known mode, such as Electronic  
3 Code Book mode.

1 36. Apparatus according to claim 24 wherein said second function includes an  
2 encryption function resulting from combined use of more than one symmetric key cipher.

1 40. Apparatus according to claim 37 wherein said first function includes a  
2 cryptographic pseudo random generator.

1 43. Apparatus according to claim 37 wherein said accessory data strings include two  
2 parts, one part being derived by the decrypting party in a predetermined fashion from  
3 available sources prior to decrypting said *i*th ciphertext segment and the other part not  
4 being derived by, and therefore being received by, the decrypting party prior to decrypting  
5 said *i*th ciphertext segment.

1 44. Apparatus according to claim 37 wherein said second function includes a  
2 decryption function of a symmetric key cipher.

1 45. Apparatus according to claim 37 wherein said second function includes a  
2 decryption function of a block cipher operating in a well known mode, such as Electronic  
3 Code Book mode.

1 46. Apparatus according to claim 37 wherein said second function includes a  
2 decryption function resulting from a combined use of more than one symmetric key cipher.

1. The first part of the paper is devoted to a general discussion of the problem of the existence of a solution of the system of equations (1) for a given set of initial conditions. It is shown that the system of equations (1) has a unique solution for a given set of initial conditions if the functions  $f_i(x, y, z, t)$  are continuous and satisfy the Lipschitz condition.

Respectfully submitted,

## ATTORNEY FOR APPLICANTS

## MARKED-UP VERSION OF AMENDMENTS

### IN THE CLAIMS:

1 1. A method of encrypting data suitable for sending to a decrypting party, said  
2 method including the steps of:

3 (a) dividing said data into data segments;

4 (b) accepting at least a cryptographic key  $k$  shared with the decrypting party;

5 (c) for the  $i$ th data segment ( $i = 1, 2, \dots$ ) to be encrypted, generating the  $i$ th  
6 segment key  $S_i$  using a first function with said cryptographic key  $k$  and some accessory  
7 data strings as inputs;

8 (d) encrypting the  $i$ th data segment using a second function with  $S_i$  as the  
9 encryption key to form the  $i$ th ciphertext segment; and

10 (e) outputting the  $i$ th ciphertext segment, and at least a part of said accessory  
11 data strings for sending data to the decrypting party, and if more data segments are to be  
12 encrypted, repeating steps (c), (d) and (e).

1 2. A method according to claim 1 wherein said accessory data strings include a single  
2 string  $V_i$  derived from the previous value  $V_{i-1}$  in a predetermined fashion.

1 3. A method according to claim 2 wherein said string  $v_i$  is derived according to the  
2 relation  $V_i = F(V_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $V_{i-1}$  to  $V_i$  and  $V_o$  is an initialization value  
3 made known to the decrypting party.

1 4. (Once Amended) A method according to claim 1[, 2 or 3] wherein step (e)  
2 includes outputting the size of the corresponding data segment.



1 5. (Once Amended) A method according [to any one of the preceding claims] claim  
2 1 wherein said first function includes a cryptographic pseudo random generator.

1 6. A method according to claim 5 wherein said pseudo random generator includes a  
2 keyed hash function  $h(k, v_{i1}, v_{i2}, \dots, v_{il})$ , wherein  $k$  is said cryptographic key,  $(v_{i1}, v_{i2}, \dots, v_{il})$   
3 is said accessory data strings and  $l$  is a positive integer.

1 7. A method according to claim 6 wherein  $h()$  is MD5 or SHA.

1 8. (Once Amended) A method according to [any one of the preceding claims] claim  
2 1 wherein said accessory data strings are derived from various sources.

1 9. A method according to claim 8 wherein said sources include current time and date,  
2 or previous accessory data strings, or some initialization values, or at least a part of the  
3 data segments or previous ciphertext segments, or at least a part of previous segment keys.

1 10. A method according to claim 1 wherein said accessory data strings include two  
2 parts, one part being derived by the decrypting party in a predetermined fashion prior to  
3 decrypting said  $i$ th ciphertext segment and the other part not being derived by, and  
4 therefore being sent to, the decrypting party prior to decrypting said  $i$ th ciphertext segment.

1 11. (Once Amended) A method according to [any one of the preceding claims] claim  
2 1 wherein said second function includes an encryption function of a symmetric key cipher.

1 12. (Once Amended) A method according to [any one of claims 1 to 10] claim 1  
2 wherein said second function includes an encryption function of a block cipher operating  
3 in a well known mode, such as Electronic Code Book mode.

1 13. (Once Amended) A method according to [any one of claims 1 to 10] claim 1  
2 wherein said second function includes an encryption function resulting from combined use  
3 of more than one symmetric key cipher.

1 14. A method of decrypting data encrypted by an encrypting party, said method  
2 including the steps of:

3 (a) accepting at least a cryptographic key  $k$  being shared with the encrypting  
4 party;

5 (b) for the  $i$ th ciphertext segment ( $i = 1, 2, \dots$ ) to be decrypted, generating the  
6  $i$ th segment key  $S_i$  using a first function with said cryptographic key  $k$  and some accessory  
7 data strings as inputs;

8 (c) decrypting the  $i$ th ciphertext segment using a second function with  $S_i$  as the  
9 decryption key;

10 (d) outputting the decrypted  $i$ th ciphertext segment, and if more ciphertext  
11 segments are to be decrypted, repeating steps (b), (c) and (d).

1 15. A method according to claim 14 wherein said accessory data strings include a  
2 single string  $V_i$  derived from the previous value  $V_{i-1}$  in a predetermined fashion.

1 16. A method according to claim 15 wherein said string  $v_i$  is derived according to the  
2 relation  $v_i = F(v_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $v_{i-1}$  to  $v_i$  and  $v_0$  is an initialization value  
3 made known to the encrypting party.

1 17. (Once Amended) A method according to claim 14[, 15 or 16] wherein said first  
2 function includes a cryptographic pseudo random generator.

1 18. A method according to claim 17 wherein said pseudo random generator includes a  
2 keyed hash function  $h(k, v_{i1}, v_{i2}, \dots, v_{il})$ , wherein  $k$  is said cryptographic key,  $(v_{i1}, v_{i2}, \dots, v_{il})$   
3 is said accessory data strings and  $l$  is a positive integer.

1 19. A method according to claim 18 wherein  $h()$  is MD5 or SHA.

1 20. (Once Amended) A method according to [any one of claims 14 to 19] claim 14  
2 wherein said accessory data strings include two parts, one part being derived by the  
3 decrypting party in a predetermined fashion from available sources prior to decrypting said  
4  $i$ th ciphertext segment and the other part not being derived by, and therefore being received  
5 by, the decrypting party prior to decrypting said  $i$ th ciphertext segment.

1 21. (Once Amended) A method according to [any one of claims 14 to 20] claim 14  
2 wherein said second function includes a decryption function of a symmetric key cipher.

1 22. (Once Amended) A method according to [any one of claims 14 to 20] claim 14  
2 wherein said second function includes a decryption function of a block cipher operating in  
3 a well known mode, such as Electronic Code Book mode.

1 23. (Once Amended) A method according to [any one of claims 14 to 20] claim 14  
2 wherein said second function includes a decryption function resulting from a combined use  
3 of more than one symmetric key cipher.

1 24. Apparatus for encrypting data suitable for sending to a decrypting party, said  
2 apparatus including:

3 (a) means for dividing said data into data segments;

4 (b) means for accepting at least a cryptographic key  $k$  shared with the  
5 decrypting party;

6 (c) means for generating for the  $i$ th data segment ( $i = 1, 2, \dots$ ) to be encrypted,  
7 the  $i$ th segment, key  $S_i$  using a first function with said cryptographic key  $k$  and some  
8 accessory data strings as inputs;

9 (d) means for encrypting the  $i$ th data segment using a second function with  $S_i$  as  
10 the encryption key to form the  $i$ th ciphertext segment; and

11 (e) means for outputting the  $i$ th ciphertext segment, and at least a part of said  
12 accessory data strings for sending data to the decrypting party.

1 25. Apparatus according to claim 24 wherein said accessory data strings include a  
2 single string  $V_i$  derived from the previous value  $V_{i-1}$  in a predetermined fashion.

1 26. Apparatus according to claim 25 wherein said string  $V_i$  is derived according to the  
2 relation  $V_i = F(V_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $V_{i-1}$  to  $V_i$  and  $V_0$  is an initialization value  
3 made known to the decrypting party.

1 27. (Once Amended) Apparatus according to claim 24[, 25 or 26] wherein said means  
2 for outputting is adapted for outputting the size of the corresponding data segment.

1 28. (Once Amended) Apparatus according to [any one of claims 24 to 27] claim 24  
2 wherein said first function includes a cryptographic pseudo random generator.

1 29. Apparatus according to claim 28 wherein said pseudo random generator includes a  
2 keyed hash function  $h(k, V_{i1}, V_{i2}, \dots, V_{il})$ , wherein  $k$  is said cryptographic key,  $(V_{i1}, V_{i2}, \dots, V_{il})$   
3 is said accessory data strings and  $l$  is a positive integer.

1 30. Apparatus according to claim 29 wherein  $h()$  is MD5 or SHA.

1 31. (Once Amended) Apparatus according to [any one of claims 24 to 29] claim 24  
2 wherein said accessory data strings are derived from various sources.

1 32. Apparatus according to claim 31 wherein said sources include current time and  
2 date, or previous accessory data strings, or some initialization values, or at least a part of  
3 the data segments or previous ciphertext segments, or a part of previous segment keys.

1 33. Apparatus according to claim 24 wherein said accessory data strings include two  
2 parts, one part being derived by the decrypting party in a predetermined fashion prior to  
3 decrypting said  $i$ th ciphertext segment and the other part not being derived by, and  
4 therefore being sent to, the decrypting party prior to decrypting said  $i$ th ciphertext segment.

1 34. (Once Amended) Apparatus according to [any one of claims 24 to 33 ] claim 24  
2 wherein said second function includes an encryption function of a symmetric key cipher.

1 35. (Once Amended) Apparatus according to [any one of claims 24 to 33] claim 24  
2 wherein said second function includes an encryption function of a block cipher operating  
3 in a well known mode, such as Electronic Code Book mode.

1 36. (Once Amended) Apparatus according to [any one of claims 24 to 33] claim 24  
2 wherein said second function includes an encryption function resulting from combined use  
3 of more than one symmetric key cipher.

1 37. Apparatus for decrypting data encrypted by an encrypting party, said apparatus  
2 including:

3 (a) means for accepting at least a cryptographic key  $k$  being shared with the  
4 encrypting party;

5 (b) means for generating as inputs for the  $i$ th ciphertext segment ( $i = 1, 2, \dots$ )  
6 to be decrypted, the  $i$ th segment key  $S_i$  using a first function with said cryptographic key  $k$   
7 and some accessory data strings;

8 (c) means for decrypting the  $i$ th ciphertext segment using a second function  
9 with  $S_i$  as the decryption key; and

10 (d) means for outputting the decrypted  $i$ th ciphertext segment.

1 38. Apparatus according to claim 37 wherein said accessory data strings include a  
2 single string  $V_i$  derived from the previous value  $V_{i-1}$  in a predetermined fashion.

1 39. Apparatus according to claim 38 wherein said string  $V_i$  is derived according to the  
2 relation  $V_i = F(V_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $V_{i-1}$  to  $V_i$  and  $V_0$  is an initialization value  
3 made known to the encrypting party.

1 40. (Once Amended) Apparatus according to claim 37[, 38 or 39] wherein said first  
2 function includes a cryptographic pseudo random generator.

1 41. Apparatus according to claim 40 wherein said pseudo random generator includes a  
2 keyed hash function  $h(k, V_{i1}, V_{i2}, \dots, V_{il})$ , wherein  $k$  is said cryptographic key,  $(V_{i1}, V_{i2}, \dots, V_{il})$   
3 is said accessory data strings and  $l$  is a positive integer.

1 42. Apparatus according to claim 41 wherein  $h()$  is MD5 or SHA.

1 43. (Once Amended) Apparatus according to [any one of claims 37 to 42] claim 37  
2 wherein said accessory data strings include two parts, one part being derived by the  
3 decrypting party in a predetermined fashion from available sources prior to decrypting said  
4  $i$ th ciphertext segment and the other part not being derived by, and therefore being received  
5 by, the decrypting party prior to decrypting said  $i$ th ciphertext segment.

1 44. (Once Amended) Apparatus according to [any one of claims 37 to 43] claim 37  
2 wherein said second function includes a decryption function of a symmetric key cipher.

1 45. (Once Amended) Apparatus according to [any one of claims 37 to 43] claim 37  
2 wherein said second function includes a decryption function of a block cipher operating in  
3 a well known mode, such as Electronic Code Book mode.





PTO/PCT Rec'd 24 SEP 2001

METHOD AND APPARATUS FOR  
ENCRYPTING AND DECRYPTING DATA

FIELD OF THE INVENTION

5

The present invention relates to cryptography and in particular to a method and apparatus for encrypting and decrypting digital data for the purpose of protecting or securing its contents.

10

BACKGROUND OF THE INVENTION

15

There exists a need to transfer data confidentially over an open channel or to store such data securely in an unsecure location. Whilst such transfer or storage may be achieved by physical means, it is more effective and/or flexible to use cryptographic means.

20

25

30

In the prior art, to send private communications between two parties, the parties need to share a cryptographic key and use a symmetric-key cipher to encrypt and decrypt data. Various ciphers including block ciphers and stream ciphers have been proposed in the past. A stream cipher handles messages of arbitrary size by ciphering individual elements, such as bits or bytes of data. This avoids the need to accumulate data into a block before ciphering as is necessary in a block cipher. A conventional block cipher requires an accumulation of a certain amount of data or multiple data elements for ciphering to complete. Examples of block ciphers include DES (see ANSI X3.92, "American National Standard for Data Encryption Algorithm (DEA)," American National Standards Institute, 1981), IDEA (see X. Lai, J. Massey, and S. Murphy, "Markov ciphers and differential cryptanalysis," Advances in Cryptology - EUROCRYPT'91 Proceedings, Springer-Verlag, 1991, pp. 17-38), SAFER (see J. Massey. SAFER K-64: One year later. In B. Preneel, editor, Fast Software Encryption - Proceedings of Second International Workshop, LNCS 1008, pages 212-241, Springer Verlag, 1995), and RC5 (see R. Rivest, "The RC5 encryption algorithm," Dr. Dobbs's Journal, Vol. 20, No. 1, January 1995, pp. 146 -148). A typical data encryption

-2-

speed for these ciphers is several million bits per second (Mb/s) on a Pentium 266 MHz processor.

5 Due to the pervasiveness of high-speed networking and multimedia communications, the demand for high-speed ciphers is ever increasing. For example, data rates over Asynchronous Data Transfer networks range from several tens of Mb/s to 1 Gb/s. Software implementations of existing block ciphers cannot reach these kinds of data rates.

10 In general, stream ciphers are much faster than block ciphers. However, stream ciphers are usually not sufficiently analyzed and are perceived to be weaker in security than block ciphers. Many stream ciphers that we believed to be very secure were subsequently broken. The design of secure and efficient high-speed ciphers remains a highly challenging problem.

15 Many powerful cryptanalytical methods have been developed during the past decade or so. It may be observed that the success of many of these methods in attacking a cipher depends on the availability of a large quantity of ciphertexts/plaintexts under a particular encryption key. Normally, the likelihood  
20 of successfully attacking a cipher, i.e., discovering the key, diminishes as the amount of available ciphertexts/plaintexts decreases. The present invention, is motivated by the above observation, and provides an improved method and apparatus for data encryption and decryption.

## 25 SUMMARY OF THE INVENTION

The method of the present invention may employ a combination of at least two cryptographic algorithms to achieve relatively high throughput without compromising security. A first algorithm may be a cryptographic pseudo random  
30 sequence (or number) generator with strong security, and a second algorithm may be a cipher capable of high-speed operation, but may be weak in security when used alone. The first algorithm may be used to systematically and periodically generate "segment keys" and the second algorithm may be used to encrypt a data segment or plaintext segment using a segment key. Each data

-3-

segment may be encrypted using a different segment key. By limiting the sizes of the data segments, an attacker may not have sufficient plaintexts or ciphertexts under a given segment key to carry out meaningful cryptanalysis against the second algorithm. In doing so, the present invention may achieve high  
5 throughput in data encryption and decryption without compromising overall security of the system.

According to one aspect of the present invention there is provided a method of encrypting data suitable for sending to a decrypting party, said method including  
10 the steps of:

- (a) dividing said data into data segments;
- (b) accepting at least a cryptographic key  $k$  shared with the decrypting party;
- (c) for the  $i$ th data segment ( $i = 1, 2, \dots$ ) to be encrypted, generating  
15 the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings as inputs;
- (d) encrypting the  $i$ th data segment using a second function with  $s_i$  as the encryption key to form the  $i$ th ciphertext segment; and
- (e) outputting the  $i$ th ciphertext segment, and at least a part of said  
20 accessory data strings for sending data to the decrypting party, and if more data segments are to be encrypted, repeating steps (c), (d) and (e).

The accessory data strings may include a single string  $v_i$  derived from the  
25 previous value  $v_{i-1}$  in a predetermined fashion. The string  $v_i$  may be derived according to the relation  $v_i = F(v_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $v_{i-1}$  to  $v_i$  and  $v_0$  is an initialization value made known to the decrypting party.

According to a further aspect of the present invention there is provided a method  
30 of decrypting data encrypted by an encrypting party, said method including the steps of:

- (a) accepting at least a cryptographic key  $k$  being shared with the encrypting party;

-4-

- 5 (b) for the  $i$ th ciphertext segment ( $i = 1, 2, \dots$ ) to be decrypted, generating the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings as inputs;
- (c) decrypting the  $i$ th ciphertext segment using a second function with  $s_i$  as the decryption key;
- (d) outputting the decrypted  $i$ th ciphertext segment, and if more ciphertext segments are to be decrypted, repeating steps (b), (c) and (d).

10 According to a still further aspect of the present invention there is provided apparatus for encrypting data suitable for sending to a decrypting party, said apparatus including:

- 15 (a) means for dividing said data into data segments;
- (b) means for accepting at least a cryptographic key  $k$  shared with the decrypting party;
- (c) means for generating for the  $i$ th data segment ( $i = 1, 2, \dots$ ) to be encrypted, the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings as inputs;
- 20 (d) means for encrypting the  $i$ th data segment using a second function with  $s_i$  as the encryption key to form the  $i$ th ciphertext segment; and
- (e) means for outputting the  $i$ th ciphertext segment, and at least a part of said accessory data strings for sending data to the decrypting party.

25 According to a still further aspect of the present invention there is provided apparatus for decrypting data encrypted by an encrypting party, said apparatus including:

- 30 (a) means for accepting at least a cryptographic key  $k$  being shared with the encrypting party;
- (b) means for generating as inputs for the  $i$ th ciphertext segment ( $i = 1, 2, \dots$ ) to be decrypted, the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings;
- (c) means for decrypting the  $i$ th ciphertext segment using a second function with  $s_i$  as the decryption key; and

-5-

- (d) means for outputting the decrypted  $\lambda$ th ciphertext segment.

The apparatus of the present invention may be conveniently embodied by means of a suitably programmed general purpose digital computer. It is well within the capability of persons skilled in the art of programming digital computers to develop software programs for implementing the encrypting/decrypting methods described herein. Alternatively the apparatus may be implemented via dedicated hardware.

## DESCRIPTION OF PREFERRED EMBODIMENT

A preferred embodiment of the present invention will now be described with reference to the accompanying drawings wherein:

FIGURE 1 depicts a flowchart of the operation of an illustrative embodiment of the present invention at the data encrypting end of a communication channel; and

FIGURE 2 depicts a flowchart of the operation of an illustrative embodiment of the present invention at the data decrypting end of a communication channel.

FIGURE 1 shows the operation of the present invention at the encrypting end of a communication channel. Data encryption is performed using two cryptographic algorithms, the first being a cryptographic pseudo random sequence generator  $R()$  and the second being a high-speed cipher  $E()$ , which may be relatively weak in security when used alone. The pseudo random sequence generator accepts two inputs  $k$  and  $v$  and outputs a pseudo random sequence  $s = R(k, v)$ . The high-speed cipher accepts a secret key  $s$  and a data segment  $d$  and produces the ciphertext  $c = E(s, d)$ . In addition, the illustrative embodiment uses a pre-determined function  $F()$  to update an initial value, i. e.,  $v_i = F(v_{i-1})$ . It is assumed that the encrypting end and decrypting ends share a secret key  $k$ , an initial value  $v_0$ , and the functions  $F()$  and  $R()$ . Moreover, it is assumed that the decrypting end knows the decrypting algorithm  $D()$  corresponding to the encrypting algorithm  $E()$ .

As shown in FIGURE 1, at step 100, a program at the encrypting end divides the data to be encrypted into segments of equal or unequal sizes:  $d_1, d_2, \dots, d_n, \dots$ . In

-6-

the former case the last segment may be padded with random data if necessary; while in the latter case, the sizes of the data segments normally need to be known by the decrypting end to facilitate decryption. Furthermore, the program accepts the shared secret key  $k$  and the shared initial value  $v_0$  as inputs, and sets the  
5 index  $i = 0$ .

At 110, the program inspects if there is any data segment available for encryption, and if not, the program terminates. Assuming that there is a data segment available, the program, at 120, increments the index  $i$  by 1, gets an updated initial  
10 value  $v_i = F(v_{i-1})$ , generates a segment key  $s_i = R(k, v_i)$ , and uses the segment key to encrypt the data segment to get the ciphertext segment  $c_i = E(s_i, d_i)$  in a manner that is well known to those skilled in the art.

At 130, the program transmits the ciphertext segment, and optionally the size of  
15 the corresponding data segment, to the decrypting end. The program then goes back to 110 to see if more data segments need to be encrypted. If so, the preceding process is repeated.

The function  $F()$  is used to update the initial value. One example is  $v_i = v_{i-1} + 1$   
20 and another example is a cryptographic hash function.

Those skilled in the art will see that the shared secret key is protected by the cryptographic pseudo random generator  $R(k, v_i)$ . To obtain good security, it is required that  $R()$  be secure against all known attacks to the key  $k$ .  $R()$  is  
25 preferably a secure one-way function or one-way hash function in  $k$ . That is, given  $R(k, v_i)$  and  $v_i$ , it should be computationally hard to find  $k$ . One example of a pseudo random generator is a keyed one-way hash function  $h(k, v_i)$  or  $h(k, p, v_i, k)$  where  $h()$  is a one-way hash function and where  $p$  pads  $k$  to a full input block as specified by some hash functions. Examples of one-way hash functions are  
30 MD5 and SHA, (refer respectively, R. Rivest, "The MD5 message digest algorithm," IETF RFC 1321, April 1992 and National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994). Another example of a cryptographic pseudo random

-7-

generator is a strong encryption algorithm such as IDEA with  $k$  as the encryption key,  $v_i$  as plaintext, and the ciphertext output as the pseudo random sequence.

In the illustrative embodiment for encryption, the segment key  $s_i$  is used by the cipher  $E()$  to encrypt only one data segment  $d_i$ . This implies that only the corresponding ciphertext segment  $c_i$  and in some cases part of the corresponding data segment are available to an attacker to cryptanalyze the cipher. One selection criteria for  $E()$  is that it should be capable of operating at a high-speed. Another selection criteria for  $E()$  is that given the limited amount of ciphertexts and even part of the corresponding data segment under a segment key, the cipher  $E()$  should be capable of resisting all known attacks. As a consequence, there is a tradeoff between the size of the data segment and system throughput; the larger the size of a data segment, the higher the throughput. On the other hand, a larger data segment implies that more ciphertexts or plaintexts under a segment key are available to an attacker to cryptanalyze the cipher  $E()$ . Examples of  $E()$  are high-speed stream ciphers or block ciphers with fewer rounds of iterations than that when they are used alone. In the latter case, the notation  $E(s_i, d_i)$  represents the encryption of data segment  $d_i$  using a block cipher even when the size of the data segment  $d_i$  is larger than the block size of the underlying block cipher and the encryption may be performed in various modes, such as Electronic Code Book or Cipher Block Chaining Mode.

One specific example of  $E()$  is the following high-speed stream cipher. Let  $N()$  be a function defined as  $N(s, x) = (((x + s_1) \oplus s_2) \times s_3) \oplus s_4) >>>$ , where  $s = s_1 s_2 s_3 s_4$  (consisting of four 32-bit strings) is a 128 bit secret key,  $x$  is a 32-bit string,  $\oplus$  is the bit-wise exclusive-or,  $+$  and  $\times$  are mod  $2^{32}$  addition and multiplication, and  $>>>$  is to reverse a 32 bit string into opposite ranking. Let  $b_1 b_2 \Lambda b_m \Lambda$  be the data to be encrypted which is a concatenation of 32 bit strings, the corresponding ciphertexts are given by  $d_i = b_i \oplus N(s, N(s, N(s, d_{i-1}) \oplus b_{i-1}) \oplus d_{i-2})$ , where the initial values  $d_{-1}, d_{-2}, d_{-3}$  can be set to  $s_2, s_3, s_4$ .

Another specific example of  $E()$  is Serpent with a reduced number of rounds. Serpent is a block cipher with 128 bit block length, variable key lengths, and 32

-8-

rounds of operations (see R. Anderson, E. Biham, and L. Knudsen, "Serpent: A Proposal for the Advanced Encryption Standard", <http://www.cl.cam.ac.uk/~ria14/serpent.html>). Its inventors showed that to attack 6 round Serpent successfully, it would require  $2^{56}$  and  $2^{116}$  plaintext blocks using linear and differential cryptanalysis, respectively. Hence, if a 6 round Serpent is used as  $E()$  to encrypt data, it should resist both linear and differential cryptanalysis as long as the data segment size is less than  $2^{56}$  128 bit blocks. At the same time, this  $E()$  is about 5 times faster than the 32 round Serpent.

10 FIGURE 2 depicts a flowchart of the operation of the present invention at the data decrypting end of a communication channel. As shown in FIGURE 2, at step 200, a program at the decrypting end accepts the shared secret key  $k$  and the shared initial value  $v_0$  as inputs, and sets the index  $i = 0$ .

15 The program then checks at 210 to see if there is any ciphertext segment available for decryption and if not, the program halts its operation. Assuming that a ciphertext segment is received, the program, at 220, increments the index  $i$  by 1, updates the initial value  $v_i = F(v_{i-1})$ , computes a segment key  $s_i = R(k, v_i)$ , and uses the segment key to decrypt the ciphertext segment to get the data segment  $d_i = D(s_i, c_i)$  in a fashion that is well known in the art.

As shown at 230, the program preferably outputs the data segment and then goes back to 210 to see if there is more ciphertext segment available for decryption. If so, the preceding steps are repeated.

25

The embodiment described above is merely one illustrative example of realizing the present invention; there can be many variants of this. For example, it is well within the capability of persons skilled in the art to suggest alternative ways of generating segment keys using a pseudo random generator, where the current segment key may depend not only on the cryptographic key  $k$ , but also on other variables such as part of the plaintext, part of the ciphertext, a time stamp, and previous segment keys.

30



Finally, it is to be understood that various alterations, modifications and/or additions may be introduced into the constructions and arrangements of parts previously described without departing from the spirit or ambit of the present invention.

CLAIMS

1. A method of encrypting data suitable for sending to a decrypting party, said  
5 method including the steps of:
- (a) dividing said data into data segments;
  - (b) accepting at least a cryptographic key  $k$  shared with the decrypting party;
  - (c) for the  $i$ th data segment ( $i = 1, 2, \dots$ ) to be encrypted, generating  
10 the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings as inputs;
  - (d) encrypting the  $i$ th data segment using a second function with  $s_i$  as the encryption key to form the  $i$ th ciphertext segment; and
  - (e) outputting the  $i$ th ciphertext segment, and at least a part of said  
15 accessory data strings for sending data to the decrypting party, and if more data segments are to be encrypted, repeating steps (c), (d) and (e).
2. A method according to claim 1 wherein said accessory data strings include  
20 a single string  $v_i$  derived from the previous value  $v_{i-1}$  in a predetermined fashion.
3. A method according to claim 2 wherein said string  $v_i$  is derived according to the relation  $v_i = F(v_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $v_{i-1}$  to  $v_i$  and  $v_0$  is an initialization value made known to the decrypting party.  
25
4. A method according to claim 1, 2 or 3 wherein step (e) includes outputting the size of the corresponding data segment.
5. A method according to any one of the preceding claims wherein said first  
30 function includes a cryptographic pseudo random generator.
6. A method according to claim 5 wherein said pseudo random generator includes a keyed hash function  $h(k, v_{i1}, v_{i2}, \dots, v_{il})$ , wherein  $k$  is said cryptographic key,  $(v_{i1}, v_{i2}, \dots, v_{il})$  is said accessory data strings and  $l$  is a positive integer.

-11-

7. A method according to claim 6 wherein  $h()$  is MD5 or SHA.
8. A method according to any one of the preceding claims wherein said  
5 accessory data strings are derived from various sources.
9. A method according to claim 8 wherein said sources include current time  
and date, or previous accessory data strings, or some initialization values, or at  
least a part of the data segments or previous ciphertext segments, or at least a  
10 part of previous segment keys.
10. A method according to claim 1 wherein said accessory data strings include  
two parts, one part being derived by the decrypting party in a predetermined  
fashion prior to decrypting said  $i$ th ciphertext segment and the other part not being  
15 derived by, and therefore being sent to, the decrypting party prior to decrypting  
said  $i$ th ciphertext segment.
11. A method according to any one of the preceding claims wherein said  
second function includes an encryption function of a symmetric key cipher.  
20
12. A method according to any one of claims 1 to 10 wherein said second  
function includes an encryption function of a block cipher operating in a well  
known mode, such as Electronic Code Book mode.
- 25 13. A method according to any one of claims 1 to 10 wherein said second  
function includes an encryption function resulting from combined use of more  
than one symmetric key cipher.
14. A method of decrypting data encrypted by an encrypting party, said  
30 method including the steps of:
- (a) accepting at least a cryptographic key  $k$  being shared with the  
encrypting party;

-12-

- (b) for the  $i$ th ciphertext segment ( $i = 1, 2, \dots$ ) to be decrypted, generating the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings as inputs;
  - (c) decrypting the  $i$ th ciphertext segment using a second function with  $s_i$  as the decryption key;
  - (d) outputting the decrypted  $i$ th ciphertext segment, and if more ciphertext segments are to be decrypted, repeating steps (b), (c) and (d).
- 10 15. A method according to claim 14 wherein said accessory data strings include a single string  $v_i$  derived from the previous value  $v_{i-1}$  in a predetermined fashion.
- 15 16. A method according to claim 15 wherein said string  $v_i$  is derived according to the relation  $v_i = F(v_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $v_{i-1}$  to  $v_i$  and  $v_0$  is an initialization value made known to the encrypting party.
- 20 17. A method according to claim 14, 15 or 16 wherein said first function includes a cryptographic pseudo random generator.
- 25 18. A method according to claim 17 wherein said pseudo random generator includes a keyed hash function  $h(k, v_{i1}, v_{i2}, \dots, v_{il})$ , wherein  $k$  is said cryptographic key,  $(v_{i1}, v_{i2}, \dots, v_{il})$  is said accessory data strings and  $l$  is a positive integer.
- 30 19. A method according to claim 18 wherein  $h()$  is MD5 or SHA.
20. A method according to any one of claims 14 to 19 wherein said accessory data strings include two parts, one part being derived by the decrypting party in a predetermined fashion from available sources prior to decrypting said  $i$ th ciphertext segment and the other part not being derived by, and therefore being received by, the decrypting party prior to decrypting said  $i$ th ciphertext segment.
21. A method according to any one of claims 14 to 20 wherein said second function includes a decryption function of a symmetric key cipher.

-13-

22. A method according to any one of claims 14 to 20 wherein said second function includes a decryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.

5

23. A method according to any one of claims 14 to 20 wherein said second function includes a decryption function resulting from a combined use of more than one symmetric key cipher.

10 24. Apparatus for encrypting data suitable for sending to a decrypting party, said apparatus including:

- (a) means for dividing said data into data segments;
- (b) means for accepting at least a cryptographic key  $k$  shared with the decrypting party;
- 15 (c) means for generating for the  $i$ th data segment ( $i = 1, 2, \dots$ ) to be encrypted, the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings as inputs;
- (d) means for encrypting the  $i$ th data segment using a second function with  $s_i$  as the encryption key to form the  $i$ th ciphertext segment; and
- 20 (e) means for outputting the  $i$ th ciphertext segment, and at least a part of said accessory data strings for sending data to the decrypting party.

25 25. Apparatus according to claim 24 wherein said accessory data strings include a single string  $v_i$  derived from the previous value  $v_{i-1}$  in a predetermined fashion.

26. Apparatus according to claim 25 wherein said string  $v_i$  is derived according to the relation  $v_i = F(v_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $v_{i-1}$  to  $v_i$  and  $v_0$  is an initialization value made known to the decrypting party.

30

27. Apparatus according to claim 24, 25 or 26 wherein said means for outputting is adapted for outputting the size of the corresponding data segment.

-14-

28. Apparatus according to any one of claims 24 to 27 wherein said first function includes a cryptographic pseudo random generator.
29. Apparatus according to claim 28 wherein said pseudo random generator  
5 includes a keyed hash function  $h(k, v_{i1}, v_{i2}, \dots, v_{il})$ , wherein  $k$  is said cryptographic key,  $(v_{i1}, v_{i2}, \dots, v_{il})$  is said accessory data strings and  $l$  is a positive integer.
30. Apparatus according to claim 29 wherein  $h()$  is MD5 or SHA.
- 10 31. Apparatus according to any one of claims 24 to 29 wherein said accessory data strings are derived from various sources.
32. Apparatus according to claim 31 wherein said sources include current time and date, or previous accessory data strings, or some initialization values, or at  
15 least a part of the data segments or previous ciphertext segments, or a part of previous segment keys.
33. Apparatus according to claim 24 wherein said accessory data strings include two parts, one part being derived by the decrypting party in a  
20 predetermined fashion prior to decrypting said  $i$ th ciphertext segment and the other part not being derived by, and therefore being sent to, the decrypting party prior to decrypting said  $i$ th ciphertext segment.
34. Apparatus according to any one of claims 24 to 33 wherein said second  
25 function includes an encryption function of a symmetric key cipher.
35. Apparatus according to any one of claims 24 to 33 wherein said second function includes an encryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.  
30
36. Apparatus according to any one of claims 24 to 33 wherein said second function includes an encryption function resulting from combined use of more than one symmetric key cipher.

-15-

37. Apparatus for decrypting data encrypted by an encrypting party, said apparatus including:

- (a) means for accepting at least a cryptographic key  $k$  being shared with the encrypting party;
- 5 (b) means for generating as inputs for the  $i$ th ciphertext segment ( $i = 1, 2, \dots$ ) to be decrypted, the  $i$ th segment key  $s_i$  using a first function with said cryptographic key  $k$  and some accessory data strings;
- (c) means for decrypting the  $i$ th ciphertext segment using a second function with  $s_i$  as the decryption key; and
- 10 (d) means for outputting the decrypted  $i$ th ciphertext segment.

38. Apparatus according to claim 37 wherein said accessory data strings include a single string  $v_i$  derived from the previous value  $v_{i-1}$  in a predetermined fashion.

39. Apparatus according to claim 38 wherein said string  $v_i$  is derived according to the relation  $v_i = F(v_{i-1})$ ,  $i = 1, 2, \dots$ , wherein  $F()$  maps  $v_{i-1}$  to  $v_i$  and  $v_0$  is an initialization value made known to the encrypting party.

40. Apparatus according to claim 37, 38 or 39 wherein said first function includes a cryptographic pseudo random generator.

41. Apparatus according to claim 40 wherein said pseudo random generator includes a keyed hash function  $h(k, v_{i1}, v_{i2}, \dots, v_{il})$ , wherein  $k$  is said cryptographic key,  $(v_{i1}, v_{i2}, \dots, v_{il})$  is said accessory data strings and  $l$  is a positive integer.

42. Apparatus according to claim 41 wherein  $h()$  is MD5 or SHA.

43. Apparatus according to any one of claims 37 to 42 wherein said accessory data strings include two parts, one part being derived by the decrypting party in a predetermined fashion from available sources prior to decrypting said  $i$ th ciphertext segment and the other part not being derived by, and therefore being received by, the decrypting party prior to decrypting said  $i$ th ciphertext segment.

-16-

44. Apparatus according to any one of claims 37 to 43 wherein said second function includes a decryption function of a symmetric key cipher.

45. Apparatus according to any one of claims 37 to 43 wherein said second  
5 function includes a decryption function of a block cipher operating in a well known mode, such as Electronic Code Book mode.

46. Apparatus according to any one of claims 37 to 43 wherein said second  
10 function includes a decryption function resulting from a combined use of more than one symmetric key cipher.



1/2

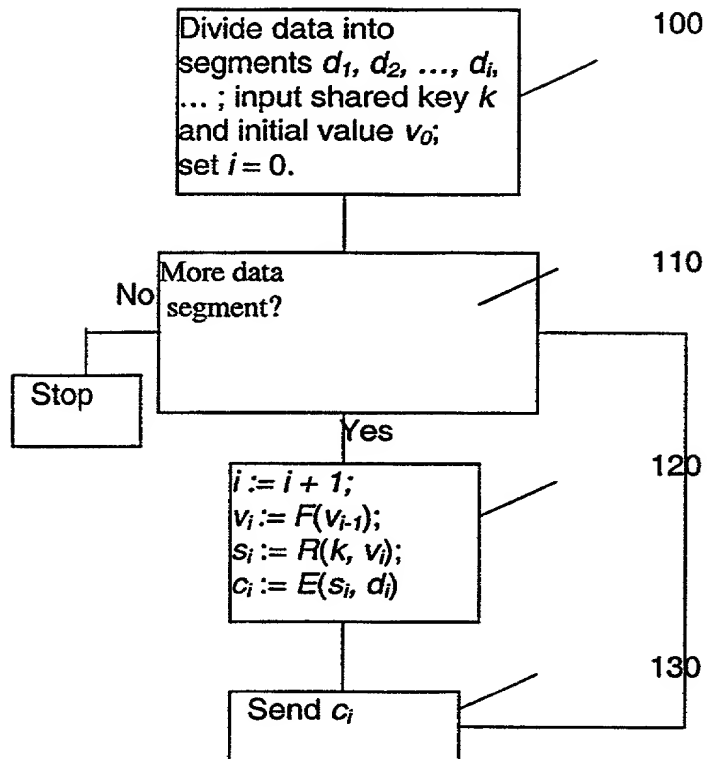
DRAWINGS

FIGURE 1

2/2

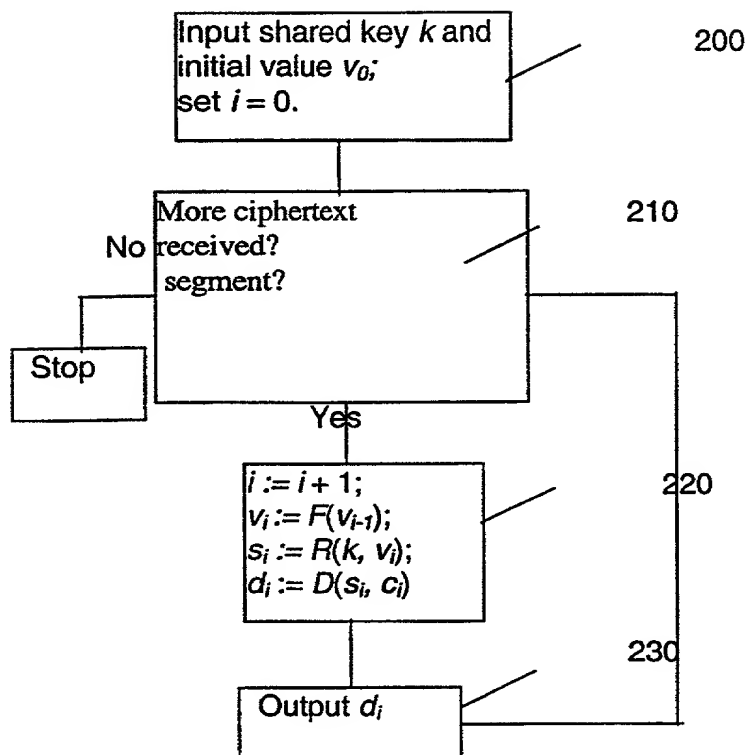


FIGURE 2

Please type a plus sign (+) inside this box → ☐

Express Mail Label No. EL915360557US

PTO/SB/01 (10-00)

Approved for use through 10/31/2002. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

**DECLARATION FOR UTILITY OR  
DESIGN  
PATENT APPLICATION  
(37 CFR 1.63)**

☒ Declaration  
Submitted  
with Initial  
Filing      OR      ☐ Declaration  
Submitted after Initial  
Filing (surcharge  
(37 CFR 1.16 (e))  
required)

**Attorney Docket Number** 2085-00100

**First Named Inventor** BAO Feng

**COMPLETE IF KNOWN**

**Application Number** NOT YET / ASSIGNED

**Filing Date** CONCURRENTLY HEREWITH

**Group Art Unit** UNKNOWN

**Examiner Name** UNKNOWN

**As a below named inventor, I hereby declare that:**

My residence, mailing address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Method And Apparatus For Encrypting And Decrypting Data

(Title of the Invention)

the specification of which

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 03/22/1999

as United States Application Number or PCT International

Application Number PCT/SG99/00020 and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box 

Express Mail Label No. EL915360557US

PTO/SB/81 (10-00)

Approved for use through 10/31/2002. OMB 0651-0035

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it display a valid OMB control number.

## POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	NOT YET ASSIGNED
Filing Date	CONCURRENTLY HEREWITH
First Named Inventor	BAO Feng
Group Art Unit	UNKNOWN
Examiner Name	UNKNOWN
Attorney Docket Number	2085-00200

I hereby appoint:

☒ Practitioners at Customer Number

23505

Place Customer  
Number Bar Code  
Label here

OR

☐ Practitioner(s) named below:

Name	Registration Number
David A. Rose	26,223
Gregory L. Maag	32,363
Michael F. Heim	32,702
Jonathan M. Harris	44,144

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☒ The above-mentioned Customer Number.

OR

☒ Firm or  
Individual Name Conely, Rose & Tayon, P.C.

Address P.O. Box 3267

Address

City Houston State TX Zip 77253-3267

Country United States of America

Telephone (713) 238 8000 Fax (713) 238 8008

I am the:

☒ Applicant/Inventor.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

### SIGNATURE of Applicant or Assignee of Record

Name DENG Huijie, Robert

Signature

Date

*Robert Deng*

4/09/2001

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

☒ \*Total of ONE (1) form is submitted.

Please type a plus sign (+) inside this box



Express Mail Label No. EL915360557US

PTO/SB/81 (10-00)

Approved for use through 10/31/2002. OMB 0651-0035

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it display a valid OMB control number.

## POWER OF ATTORNEY OR AUTHORIZATION OF AGENT

Application Number	NOT YET ASSIGNED
Filing Date	CONCURRENTLY HEREWITH
First Named Inventor	BAO Feng
Group Art Unit	UNKNOWN
Examiner Name	UNKNOWN
Attorney Docket Number	2085-00200

I hereby appoint:

☒ Practitioners at Customer Number

23505

Place Customer  
Number Bar Code  
Label here

OR

☐ Practitioner(s) named below:

Name	Registration Number
David A. Rose	26,223
Gregory L. Maag	32,363
Michael F. Heim	32,702
Jonathan M. Harris	44,144

as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Please change the correspondence address for the above-identified application to:

☒ The above-mentioned Customer Number.

OR

☒ Firm or  
Individual Name Conely, Rose & Tayon, P.C.

Address P.O. Box 3267

Address

City

Houston

State

TX

Zip

77253-3267

Country

United States of America

Telephone

(713) 238 8000

Fax

(713) 238 8008

I am the:

☒ Applicant/Inventor.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

### SIGNATURE of Applicant or Assignee of Record

Name

BAO Feng

Signature

x [Signature]

Date

x 04/09/2001

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

☒ \*Total of Three (3) form is submitted.

Burden Hour Statement: This form is estimated to take 3 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (10-00)

Approved for use through 10/31/2002. OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

## DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☒ Customer Number or Bar Code Label ☐ Correspondence address below

23505

Name

Address

Address

City

State

ZIP

Country

Telephone

Fax

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR :

☐ A petition has been filed for this unsigned inventor

Given Name

Feng

(first and middle [if any])

Family Name  
or Surname

BAO

Inventor's  
Signature

Date

04/09/2001

Residence: City

Singapore

State

Country

SG

Citizenship

P.R.China

Mailing Address

37 West Coast Park, #04-06, Parkview Condo

Mailing Address

City

Singapore

State

ZIP

127653

Country

Singapore

NAME OF SECOND INVENTOR:

☐ A petition has been filed for this unsigned inventor

Given Name

Huijie, Robert

(first and middle [if any])

Family Name  
or Surname

DENG

Inventor's  
Signature

Date

4/09/2001

Residence: City

Singapore

State

Country

SG

Citizenship

Singapore

Mailing Address

2 Namly Rise

Mailing Address

City

Singapore

State

ZIP

267110

Country

Singapore

☐ Additional inventors are being named on the \_\_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.